10. National Security Strategic Goal

"Ensure the security of the transportation system for the movement of people and goods, and support the National Security Strategy"

10.1 Outcomes

1. Reduce the vulnerability of the transportation system and its users to crime and terrorism

2. Increase the capability of the transportation system to meet national defense needs

3. Reduce the flow of illegal drugs entering the United States

4. Reduce the flow of migrants illegally entering the United States

5. Reduce illegal incursions into our sovereign territory

6. Increase support for United States interests in promoting regional stability

7. Reduce transportation-related dependence on foreign fuel supplies

10.2 Strategies

DOT's national security strategies show how we will address security threats that have existed for a long time as well as threats that have emerged more recently. They reflect our ONE DOT philosophy which stresses partnerships, collaboration and taking steps to create a climate of innovation. They address military contingencies, disaster response, drugs, illegal migration, and new communications technologies. Security is an important aspect of transportation: transportation is the vital link to mobilizing materials and our armed forces to defend the nation; and transportation is first in the civilian emergency response action agenda.

As we move into the information age, we are increasingly concerned with security strategies that address information assurance and protection. Those efforts reflecting DOT's partnerships with the transportation industry to protect command and control and communications systems are addressed in the national security section of the plan. However, strategies that reflect DOT's commitment to protect internal information systems and DOT's information assets are presented under the organizational excellence section.[1]

DOT will employ six key strategies to achieve our National Security outcomes. We will: 1) take several steps to protect the transportation system from security threats; 2) secure the borders of

[1] See section 11.2

the United States; 3) foster public awareness and acceptance of transportation security; 4) promote international standards for transportation security; 5) support the development of new security technologies; and 6) share timely information on security issues with stakeholders.

In contrast to the DOT safety strategies all of which supported our safety outcomes of reduced fatalities and injuries, our national security strategies are targeted to specific outcomes. The resources and programs listed in DOT's Annual Performance Plan and budget are necessary to achieve the national security outcomes presented above and execute the strategies presented below. Each year, DOT reassesses its performance goals and targets based upon appropriations. The schedule for executing the strategies extends from the present through 2005. With respect to processes and technology, we will continue to benchmark and improve processes and move quickly toward electronic government to improve our efficiency and customer service.

10.2.1 Infrastructure Strategies: Work in partnership with other federal agencies, state and local governments, international organizations, and the private sector to:

a. Identify and reduce the vulnerabilities of all modes of transportation to security threats; (Supports outcomes 1 and 2)
b. Detect and counter threats to the security of the transportation system; (Supports outcomes 1 and 2)
c. Ensure that the national transportation system maintains the resources and capacity needed to support national defense requirements and assist in disaster response and recovery efforts; (Supports outcomes 2 and 5)
d. Develop, test and evaluate plans for the expeditious and efficient intermodal movement of personnel and materiel from origin to destination during military contingencies and disaster response; (Supports outcome 2)
e. Work in partnership with other federal agencies, state and local government, international organizations, and the private sector to implement an integrated transportation security R&D program tailored to threats and vulnerabilities including software assurance, high confidence systems, and real-time chemical and biological detection; (Supports outcomes 1 and 2)
f. Promote performance-based standards developed in close coordination with industry to address their cost, throughput and portability needs; and
g. Advance cost-shared, public-private partnerships to accelerate the development, demonstration and deployment of new security technologies and systems. (Supports outcomes 1 and 2)

10.2.2 Strategies to Secure U.S. Borders: Work in partnership with federal agencies, state and local governments to optimize the use of DOT assets and increase the effectiveness of procedures, protocols and communications to :

a. Reduce the flow of illegal drugs into the U.S.; and (Supports outcomes 3 and 5)
b. Reduce the flow of migrants illegally entering the U.S. (Supports outcomes 4 and 5)

10.2.3 Customer Focus and Communications Strategies:

a. Promote education and outreach programs designed to foster an awareness and acceptance of effective security measures within all transportation modes in collaboration with a wide range of public and private organizations. (Supports outcomes 1, 3 and 4)
b. Employ advancements in communications technology to improve the speed, accuracy and simplicity of the exchange of security, emergency response, and defense deployment information with federal, state and local governments and the private sector. (Supports outcomes 1-7)

c. Provide nation-building assistance in support of U.S. foreign policy to help foreign governments improve their critical security and transportation infrastructures. (Supports outcomes 1 and 6)

10.2.4 Guidelines, Best Practices and Standards Strategies: Establish public/private partnerships to :

a. Develop and promulgate domestic and international transportation security guidelines, recommended procedures, best practices and standards; and . (Supports outcomes 1 - 7)
b. Support or propose legislation designed to safeguard the Nation against criminal and terrorist activity in the transportation sector. (Supports outcomes 1 - 7)

10.2.5 Research and Development Strategies: Work in partnership with other Federal agencies, state and local government, international organizations, and the private sector to:

a. Support and implement an integrated transportation security R&D program tailored to threats and vulnerabilities in all modes that includes software assurance, high confidence systems and real time chemical and biological detection; (Supports outcomes 1 and 2)
b. Support development of new technologies to detect, disrupt and deter the illegal transportation of drugs and illegal migrants into and within the U.S. and at U.S. borders; and (Supports outcomes 3, 4 and 5)
c. Promote research and development on alternative energy sources and the use of energy efficient technologies. (Supports outcome 7)

10.2.6 Information and Analysis Strategies: Collect and share information on security issues and trends with those who can improve the security of the transportation system and advance our national security interests through:

a. Use of web-enabled and other technologies to improve the timeliness, validity and reliability of transportation data related to security; (Supports outcomes 1 - 7)
b. Collection, analysis and publication of data and information to identify and update critical security and national security trends and issues using formats understandable to security specialists and to the public; and (Supports outcomes 1 - 7)
c. Creation of an industry-DOT partnership to resolve information sharing issues, and to develop standards, best practices and guidelines for performance measurement. (Supports outcomes 1 - 7)

10.3 Management Challenges

The strategies outlined in the previous section represent our approach to the performance challenges of the future. However, we acknowledge that achievement of our National Security outcomes is contingent upon resolving the priority management issues identified by the GAO and DOT's OIG. The OIG identified management challenges affecting transportation and computer security, including the security of aviation, surface transportation, and critical information technology (IT) assets. The language that describes each challenge is essentially the language used by the OIG.

10.3.1 Transportation Security

The OIG has noted that DOT needs to ensure that the transportation system is secure. He observed that the changing threat of terrorist and other criminal activities has heightened the need to improve domestic transportation security.

DOT has acknowledged the changing nature of transportation security and the increasing importance of security issues by creating a stand-alone national security strategic goal in its 1997 Strategic Plan. Previously, DOT had considered security as part of transportation safety. In the three years since the 1997 Plan was published, security has taken on new, even menacing, global dimensions. Although addressing security issues has become even more crucial to DOT, several important management challenges require attention.

Aviation

The FAA has acknowledged the security challenge. Following the recommendations of the White House Commission on Aviation Safety and Security, FAA will expand its research to develop better technology and procedures to prevent weapons and explosive devices from being taken aboard commercial aircraft. Working with airlines and airports, FAA will continue to purchase and deploy advanced aviation security equipment, monitor its use, and test and assess performance of security programs including access control and cargo. The planned certification of screening companies is expected to increase levels of screener professionalism. FAA will continue to promote formation of airport security consortia. The performance-based approach to industry compliance with security requirements will encourage partnering to improve aviation security. The following milestones address challenges in aviation security in support of outcome 1.

> *Milestone: FAA will publish a final rule setting performance standards for certification of security screening companies based on the ability to identify threat objects projected onto screens using Threat Image Projection (TIP). (FY 2001)*
>
> *Milestone: FAA will begin certifying screening companies using the rule. (FY 2002)*
>
> *Milestone: FAA will continue purchase and deployment of explosives detection systems, explosives trace detection devices, and other advanced security technologies. (Ongoing; number to be purchased and installed vary by year.)*
>
> *Milestone: FAA will publish a Final Rule requiring automated passenger screening using the Computer-Assisted Passenger Prescreening System (CAPPS) with bag match or, where available, explosives detection system (EDS) screening of selected passengers' bags. (FY 2001).*

Milestone: FAA will assess facility security at all FAA Level 1-4 facilities and achieve physical security accreditation for at least 23 facilities. (FY 2002)

Surface Transportation

DOT has acknowledged the challenge the changing threat of terrorist and other criminal activities and is currently developing a surface transportation security strategy, as recommended by both the National Research Council and the DOT OIG. This document will define the surface transportation security problem and the Department's security objectives as well as identify DOT's role in such efforts as security R&D. To address these concerns, DOT will achieve the following milestone in support of outcome 1.

Milestone: The strategy will be completed by September 2000.

The transportation industry is reluctant to share proprietary and sensitive security information with the Department as it is subject to public disclosure under the Freedom of Information Act (FOIA). Conversely, assigning a security classification to information, such as risk or vulnerability assessments, by DOT as a protective measure prevents the sharing of results with industry officials, most of whom do not hold clearances. In addition, DOT lacks statutory and regulatory authority to require data collection, or to mandate security standards for the surface transportation system. Understanding these limitations, DOT must work to establish an industry Sector Coordinator who will facilitate cooperative industry-DOT partnerships to resolve information sharing issues, and to consider a set of security standards, best practices, and guidelines. Discussions with industry partners as to who will take on the role of Sector Coordinator are ongoing. DOT hopes to have a commitment by September 2000. Once these partnerships are established, performance issues in security can be more effectively addressed.

Milestone: Commitment on Sector Coordinator(s) September 2000.

10.3.2 Computer Security

DOT has acknowledged the computer security challenge. In response to Presidential Decision Directive 63 (PDD-63), which requires the federal government to achieve and maintain the ability to protect our nation's critical infrastructure by 2003, DOT has identified its critical IT assets as residing within the FAA and US Coast Guard.[2] Critical IT assets have been identified and plans are under development to evaluate, remediate, test and certify these systems in accordance with existing federal IT security policy and guidance.[3] Risk assessments are an important step in this process and will be conducted for all PDD-63 systems. These and other steps will ensure that DOT systems are adequately protected by the deadline of May 2003. While FAA and USCG are the only DOT operating administrations (OA's) that have IT assets that meet the criteria of PDD-63, other OA's are developing plans to assess their assets as required by OMB Circular A-130. DOT has established an IT Security Policy that requires all DOT IT systems be assessed to identify vulnerabilities, evaluate and mitigate these where justified, and then test and certify

[2] No other DOT systems meet the criteria of PDD-63.

[3] Computer Security Act of 1987, OMB Circular A-130, PDD-63, NIST guidance, etc.

that adequate protection has been implemented.[4] To address these security concerns, DOT will achieve the following milestones in support of outcome 1:

> *Milestone: Distribute an approved FAA Order and an FAA Information Security Concept of Operations, finalize a long term plan for deployment of Computer Security Incident Response Capability (CSIRC), and ensure that 100 percent of FAA employees receive general security awareness training and 60 percent of systems administrators receive specialized security training. (FY 2000)*
> *Milestone: FAA will enhance CSIRC and achieve a 20 percent increase in systems completing vulnerability assessments and a 10 percent increase in systems obtaining security certification and authorization. (FY 2001)*
> *Milestone: The DOT Critical Infrastructure Protection Plan (CIPP) sets out a remediation schedule for critical IT assets including risk assessment and development of security and contingency plans, a security training program, and a recruitment/retention/education/evaluation plan. Consistent with the DOT CIPP, USCG has developed its Critical Infrastructure Remediation Plan (CIRP) for its critical IT assets that include one facility, the Operations Systems Center (OSC), and five systems.*
> *Milestone: The OSC risk assessment was completed September 1999. Risk assessments for several of the critical systems have been completed. All risk assessments will be completed by November 2000.*
> *Milestone: The Security Plan for OSC was completed in March 2000. The Security Plans for all critical systems will be completed by April 2001.*
> *Milestone: OSC Contingency Plan is on schedule for completion by June 2001. Contingency Plans for all critical systems will be completed by April 2001.*
> *Milestone: Security Training Programs for OSC and all critical systems are already in place.*

10.3.3 Coast Guard Deepwater Capability Replacement Project

The $9.8 to $15 billion, 20-year Deepwater Project is the largest capital improvement project ever undertaken by the USCG. The OIG has acknowledged that the USCG is using an innovative planning process and that when completed it should provide a good basis for establishing needs and developing an acquisition strategy. However, the OIG has stated that there are several critical challenges remaining to ensure that the Deepwater Project is justified and affordable. The USCG needs to fill gaps in the planning process and respond to concerns about how it can proceed with a request to start buying assets in advance of completing its comprehensive planning process. Also, USCG still needs to develop reliable cost estimates, avoid problems other agencies have encountered in major-system replacements, and be realistic about competing budget demands from other DOT agencies.

The USCG has acknowledged this management challenge. In its report of January 2000, the Interagency Task Force on Roles and Missions validated USCG missions, and confirmed ongoing or increasing demand for future USCG services. The USCG has undertaken the recapitalization of its assets in the deepwater operating environment. The Deepwater Capability Replacement Project will see the performance-based acquisition of assets to perform USCG deepwater missions

[4] See Organizational Excellence Section 11.3.1.

worldwide. Working with industry teams, the USCG will acquire an integrated system of surface, air, command and control, intelligence and logistics systems. The conceptual design phase of the project was completed in December 1999. Additional milestones are presented below in support of outcomes 1-6.

Milestone: Complete functional design of project (April 2001)
Milestone: Update Legacy Asset Baseline[5] (June 2000)
Milestone: Begin preparing the Request for Proposal for build-out of the system (November 2000).
Milestone: Complete functional design implementation plan (April 2001)
Milestone: Issue Request for Proposal (May 2001)
Milestone: Receive proposals from industry teams (July 2001)
Milestone: Announce contract award (January 2002)

10.4 Completed Program Evaluations

DOT has evaluated a key program to determine the best allocation of resources to Coast Guard shore stations. The results of this evaluation are presented below.

10.4.1 Shore-Based Response Boat Force Mix Study (USCG 1999): This evaluation assessed whether USCG small boats are allocated to shore stations in the most effective and efficient manner. Findings indicate that the majority of Coast Guard shore stations have a shortage, and a few stations have excess small boat capability which can be reallocated to stations facing shortages. Based on the results, the Coast Guard will ensure the most effective allocation of capability to provide better overall value to the public from available resources in support of strategy 10.2.1.c and outcomes 3, 4, and 5.

10.5 External Factors

DOT used four scenarios[6] in the planning process to illustrate how external factors might impact transportation security in the next 30 years. Globalization, demographics, the U.S. economy and the role of government were the major dimensions of the scenarios. We learned that these and several other external factors such as regional instability, cargo and human smuggling, web-enabled communication and international cooperation may play a part in DOT's ability to achieve our national security outcomes. Within the U.S., the private sector and state and local agencies own and operate much of the Nation's transportation infrastructure and their cooperation is vital in ensuring the security of the transportation system. Unable to predict how these externalities may interact with one another or how they may effect our ability to achieve our national security outcomes, we have outlined both the positive and negative impacts of these factors.

10.5.1 Economic Factors

A strong national economy, corporate mergers and consolidations, and increased global competition could impact the readiness and capability of the transportation infrastructure to meet national security objectives. (Impacts outcomes 2, 6 and 7)

[5] The Legacy Asset Baseline documents maintenance events and backlogs planned.
[6] DOT's global transportation scenarios are at www.dot.gov/stratplan

Growth in volumes of people and goods moving across borders will make it increasingly difficult to detect and separate illegitimate from legitimate activities. (Impacts outcomes 1 and 4)

Large increases in the cost of fuel could stress portions of the transportation system and potentially make lower cost, more frequently used modes more likely targets for criminal and terrorist activity. (Impacts outcomes 1 and 7)

Socioeconomic and political conditions, both here and abroad will influence the criminal actions of those who profit from moving illegal drugs and other contraband into and within the United States. (Impacts outcome 3)

Tight labor markets in a strong national economy and could make recruiting and retention of personnel in critical security disciplines difficult. (Impacts outcomes 1-6)

10.5.2 Technological Factors

Combating the increasing sophistication of devices and techniques that terrorists and criminals may use to threaten or impinge upon the security of the U.S. transportation system and its lines of communication will require advances in technology and human vigilance. (Impacts outcome 1)

More drugs, contraband and even people will be smuggled via commercial cargo containers. Technologies capable of tagging and tracking will be needed to facilitate real-time surveillance and scanning of carriers and cargoes to improve contraband detection. (Impacts outcomes 3, 4, 5 and 6)

Detection technology developed for and used by aviation may not lend itself well to other transportation systems. Systems that are used for commuter transport have higher volumes of passengers using the systems during more compressed timeframes. Therefore, these systems may require technology with high specificity and lower alarm rates to maintain passenger throughput. (Impacts outcomes 1 and 3)

10.5.3 Political Factors

Nation states will provide the basic geopolitical framework, but boundaries will continue to blur with the emergence of novel economic and security relationships. Greater numbers of powerful non-state entities with diverse interests and communications via the Internet will influence the global community. (Impacts outcomes 1-6)

Improved intelligence and surveillance capabilities will yield increased, and more timely threat information. Private transportation providers and public authorities will need to maintain the flexibility and willingness to adjust security and transport procedures based on threat information. (Impacts outcomes 1, 2, 5 and 6)

The sharing of proprietary and sensitive security information between public authorities and industry officials will be increasingly important to meeting future transportation security challenges. DOT and industry will have to explore new, non-traditional approaches for sharing sensitive information, overcoming disclosure concerns presented by the Freedom of Information Act, and national security clearance limitations. (Impacts outcome 1)

The ability to improve transportation security internationally will be dependent on the extent to which other countries collaborate with or impede U.S. assessments of their seaport and airport security. (Impacts outcomes 1, 5 and 6)

Regional instabilities could lead to attacks on U.S. interests including transportation. (Impacts outcomes 1, 5 and 6)

Increased involvement of organized, professional smugglers represents a significant change in the illegal migrant threat. With more resources at their disposal than individual migrants, smugglers will employ more sophisticated techniques and the latest technology to avoid detection and thwart law enforcement efforts. (Impacts outcome 4)

10.5.4 Environmental Factors

Increasing demand for food, especially protein, and water along with public sensitivity to environmental issues will prompt protective actions to prevent over exploitation of the sea's and fresh water resources. High-sea's migratory species will require cooperative international and regional protection. (Impacts outcomes 5, 6 and 7)

Increased need for energy may stimulate oil and gas drilling in areas beyond the U.S. continental shelf more than 350 miles offshore and in depths greater than 2,000 feet. (Impacts outcome 7)

10.5.5 Social Factors

Public expectation for increased reliability and throughput and reduced transportation times will need to be balanced with requirements for passenger and transportation system security. (Impacts outcomes 1 and 3)

Public tolerance of security measures in aviation is relatively higher due to the perceived threat to this mode, a history of attacks, and the infrequency of airline travel by most Americans as compared with other modes. Should threats to other modes of transportation increase, DOT will have the challenge of addressing a low public tolerance of additional security measures on a frequent, even daily, commuter basis. (Impacts outcome 1)

10.6 Relationship Between Strategic Plan Outcomes and Performance Plan Candidate Measures

Each national security outcome in this Strategic Plan for 2000-2005 will be supported by one or more national security performance measures fully developed in DOT's Annual Performance Plans for the fiscal years 2002-2005. For example, our results in achieving the outcome *Reduce the vulnerability of the transportation system and its users to crime and terrorism* will be gauged, in part, by progress or milestones in improving the detection rate for simulated explosives that may be brought aboard aircraft. In the national security strategic goal there are three outcomes that were not in DOT's 1997-2002 Strategic Plan. We have discussed this issue at some length during the planning process and understand that we need to develop performance measures for these new outcomes.

DOT's Annual Performance Reports will provide targets, narrative and quantitative information on the extent to which we have achieved each of our national security outcomes. Table 10.6 illustrates the relationships between the outcomes in the Strategic Plan and the measures in the Performance Plan. The measures presented in Table 10.6 are candidates for the Performance Plan and are not final selections.

Table 10.6 National Security Strategic Goal, Outcomes and Performance Plan Candidate Measures

"Ensure the security of the transportation system for the movement of people and goods, and support the National Security Strategy"

Outcomes	Performance Plan Candidate Measures
Reduce the vulnerability of the transportation system and its users to crime and terrorism	Vulnerability to Crime and Terrorism Detection rate for explosives and weapons that may be brought aboard aircraft
Increase the capability of the transportation system to meet national defense needs	Of those who need to act, percent that receive threat information within 24 hours
Reduce the flow of illegal drugs entering the U.S.	National Defense Percentage of days that the designated number of critical defense assets maintain combat readiness rating of 2
Reduce the flow of migrants illegally entering the U.S.	Ship capacity available to meet DOD's requirements for intermodal sealift capacity
Reduce illegal incursions into our sovereign territory	Of the mariners needed to crew combined sealift and commercial fleets during national emergencies, the percent of the total that are available
Increase support for United States interests in promoting regional stability	Drugs Seizure rate for cocaine that is shipped through transit zone
Reduce transportation-related dependence on foreign fuel supplies in support of the National Security Strategy	Migrants Success rate for undocumented migrants attempting to enter the U.S. over maritime routes
	Incursions To Be Determined Coast Guard
	Regional Stability To Be Determined Office of Intelligence and Security
	Dependence on foreign fuel Transportation energy consumption (in quadrillion BTUs) per trillion dollars of real GDP

10.7 Data Capacity

The candidate performance measures in Table 10.6 above include measures utilized in DOT's 2001 Performance Plan and new candidate measures. DOT has developed data for each measure and has published source and accuracy statements for each of the data systems used for constructing these measures.[7] We have described the scope of each measure, the limitations of the data and the statistical issues regarding uncertainty in the measurement.[8] Led by the Bureau of Transportation Statistics (BTS), DOT's Operating Administrations are implementing a plan for verification and validation of all departmental data used in implementing GPRA and for other analytical purposes.[9] DOT is committed to continuous improvement in the accuracy, reliability and timeliness of transportation security data and is addressing the data needs described below.

[7] See www.bts.gov
[8] See Appendix I DOT 2001 Performance Plan
[9] See page 161 DOT 2001 Performance Plan

Data Needs for National Security
Existing information sources provide indicators for many of the performance measures associated with the National Security Goal. However, in some cases, the data necessary for the Department to measure its attainment of some outcome goals and strategies is lacking, or, in certain instances, no data currently exists. DOT will strive, during the course of this Strategic Plan, to address the following deficiencies in measurement data. Resources permitting, we will: 1) develop better and more complete exposure data for drug and alien interdiction programs; 2) Develop data sources addressing national security concerns associated with the transportation system's dependence on and disruptions to foreign fuel supplies; and 3) improve data on the vulnerability of the transportation system to intentional acts of disruption or destruction.

The Department holds no reliable data on the vulnerability of the nation's transportation system for a variety of reasons. For the most part, the Department lacks statutory and regulatory authority to require data collection, or to mandate security standards for the surface transportation system. The Freedom of Information Act (FOIA) effectively prevents the Department from protecting sensitive industry security data even if industry shared that data. Understanding these limitations, DOT must first establish an industry Sector Coordinator. DOT may then establish an industry-DOT partnership to resolve the many information sharing issues, and to consider development of a set of security standards, best practices, and guidelines that may then form the basis for performance measurement.

10.8 Cross-Cutting Programs

DOT has significant alliances and high-level collaboration with several other federal agencies in the security area. DOT staff communicates and meets with other agencies to align policies, process, field work and procedures that advance these initiatives. Below we present partnerships that are most directly aligned with and supportive of our national security strategic goal and outcomes.

10.8.1 Aviation Security

Goal: Prevent explosives, weapons and other dangerous items from being placed aboard aircraft. (Supports outcome 1)
Agencies Involved: DOT/FAA lead, Federal Bureau of Investigation, Bureau of Alcohol, Tobacco and Firearms, U.S. Customs Service, U.S. Postal Service, airport authorities and U.S. and foreign carriers.

10.8.2 Seaport Security

Goal: Assess and monitor port and waterway vulnerabilities, and respond to threats to seaport security. (Supports outcomes 1, 2 and 3)
Agencies Involved: DOT/USCG lead, MARAD, U.S. Customs Service, Department of the Navy, state and local port authorities.

10.8.3 Drug Interdiction

Goal: Reduce the flow of illegal drugs entering the United States. (Supports outcome 3)
Agencies Involved: DOT/USCG lead, FMSCA, FAA, Office of National Drug Control Policy, Drug Enforcement Agency, Department of Defense, U.S. Customs Service, Department of State, Federal Bureau of Investigation.

10.8.4 Migrant Interdiction

Goal: Reduce flow of illegal migrants entering the United States. (Supports outcome 4)

Agencies Involved: DOT/USCG lead, FMCSA, Immigration and Naturalization Service, Departments of State and Defense, U.S. Customs Service, U.S. Border Patrol, foreign governments, state and local enforcement authorities.

10.8.5 Marine Resource Protection
Goal: Protect living marine resources within the U.S. EEZ and in international waters in support of public law and international agreements and conventions. (Supports outcome 5)
Agencies Involved: DOT/USCG lead, National Marine Fisheries Service, Regional Fishery Management Councils, international governing bodies, foreign governments, state and local authorities.

10.8.6 Defense Sealift Capacity
Goal: Maintain sufficient capacity and crews to meet DOD surge and sustainment requirements during a national emergency. (Supports outcome 2)
Agencies Involved: DOT/MARAD lead, Department of Defense, U.S. maritime industry.

10.8.7 Port Readiness
Goal: Timely availability of DOD-designated commercial port facilities for the embarkation of military equipment and supplies during mobilizations. (Supports outcome 2)
Agencies Involved: DOT/MARAD lead, USCG, Department of Defense, U.S. port industry.

10.8.8 Chemical and Biological Weapons Detection
Goal: Evaluate chemical and biological detection systems for use in the special environments of transit passenger terminals. (Supports outcome 1)
Agencies Involved: DOT/FTA lead, Department of Energy, Washington, D.C. Metropolitan Area Transit Authority (WMATA).

10.8.9 Intelligence
Goal: Obtain, analyze, and disseminate information on threats to the nation and our critical infrastructure. (Supports outcome 1)
Agencies Involved: DOT/USCG lead, FAA, Central Intelligence Agency, National Security Agency, National Intelligence Council, Defense Intelligence Agency, Federal Bureau of Investigation, state and local law enforcement.

10.8.10 National Defense
Goal: Ensure interoperability of systems and maintain a state of readiness (e.g., sufficient capacity and personnel) to defend the nation in time of war. (Supports outcome 2)
Agencies Involved: DOT/USCG lead, MARAD, Department of Defense, National Guard.

10.8.11 Critical Infrastructure Protection

Goal: Achieve and maintain the ability to protect our nation's critical transportation infrastructure by 2003, per Presidential Decision Directive (PPD) 63. (Supports outcome 1)

Agencies Involved: DOT/Office of Intelligence and Security lead, all DOT Operating Administrations, National Security Council, Department of Defense, National Infrastructure Protection Center, Critical Infrastructure Assurance Office, transportation industry, state and local governments.

10.8.12 Regional Stability

Goal: Provide nation-building assistance in support of U.S. foreign policy to help foreign governments improve their critical security and transportation infrastructures. (Supports outcomes 1 and 6)

Agencies Involved: DOT/USCG lead, Departments of Defense, Treasury Justice, Agency for International Development, Security Assistance Program, International Maritime Organization, foreign governments.